Last Time: Proved [Quotient-Remainder Theorem]

↳ Actually proved special case: $n, d \in \mathbb{N}_0$.

↳ Extend this result to $\mathbb{Z}$ as an exercise.

↳ Sometimes called the "Division Algorithm".

Consequences of QRT

I. Modular Arithmetic.

modulus...

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}_+$.

a, b both have remainders modulo m...

Idea: Identify a, b w/ remainders ...

denote by $n \equiv a \bmod m$.

Defn: The class of $a \in \mathbb{Z}$ modulo m is

$$[a]_m \overset{*}{=} \{n \in \mathbb{Z} : n \text{ and } a \text{ have the same remainder modulo } m\}.$$

$$= \{n \in \mathbb{Z} : n \equiv a \bmod m\}$$

we need to understand this...

Let $\mathbb{Z}/m\mathbb{Z} := \{[n]_m : n \in \mathbb{Z}\}$ for any $m \in \mathbb{Z}_+$

Ultimate Claim: There is a natural arithmetic on $\mathbb{Z}/m\mathbb{Z}$ (induced by arithmetic on $\mathbb{Z}$).

Prop: Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}_+$. The following are equivalent.

① a and b both have the same remainder modulo m.

② $[a]_m = [b]_m$

③ $m \mid (b - a)$

QRT: Given $n, d \in \mathbb{Z}$ w/ $d > 0$, there exist unique $q, r \in \mathbb{Z}$ satisfying both $n = dq + r$ and $0 \le r < d$.

pf: Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}_+$.

① → ②: Suppose a and b have the same remainder mod m. (WTS: $[a]_m = [b]_m$) Let $n \in [a]_m$. Thus n has the same remainder r as a mod m. As a has the same remainder as b mod m, b also has remainder r mod m, Thus n has the same remainder as b mod m, so $n \in [b]_m$. Thus $[a]_m \subseteq [b]_m$. By symmetry of "same remainder", we see $[b]_m \subseteq [a]_m$ also holds. Hence $[a]_m = [b]_m$.

② → ③: Assume $[a]_m = [b]_m$. (WTS: $m \mid (b-a)$). Because $a \in [a]_m = [b]_m$, we see a and b have the same remainder mod m. In particular, there are $q, q', r \in \mathbb{Z}$ w/ $a = mq + r$ and $b = mq' + r$ and $0 \le r < m$ by the QRT. Now

$$b - a = (mq' + r) - (mq + r) = m(q' - q) + (r - r) = m(q' - q)$$

and $q' - q \in \mathbb{Z}$ by closure of $\mathbb{Z}$ under subtraction, so $m \mid (b-a)$ by definition of divisibility.

③ → ①: Assume $m \mid (b-a)$. (WTS: b and a have same remainder modulo m). By definition of divisibility there is $k \in \mathbb{Z}$ such that $b - a = mk$. By the QRT, there exist $q, r \in \mathbb{Z}$ w/ $a = mq + r$ and $0 \le r < m$.

$\therefore b = mk + a = mk + (mq + r) = m(k + q) + r$ by basic arithmetic. By uniqueness in QRT, r is the remainder of b under division by m. Hence a, b have the same remainder mod m.

Hence the original statement holds. ☑

Cor: Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}_+$. We have $a \equiv b \bmod m$ if and only if $m \mid (b-a)$.

pf: This is ① ↔ ③ rewritten using congruence notation ☑

Defn: Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}_+$. Define

$$[a]_m + [b]_m := [a+b]_m \quad \text{and}$$

$$[a]_m \cdot [b]_m := [a \cdot b]_m$$

"Cayley Tables"

Ex: Let's compute Operation Tables for $+$ and $\cdot$ mod 5.

Convention: we'll write the remainder to stand for its class.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	(3)

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	(2)	1

Ex: $[4]_5 + [4]_5 = [4+4]_5$
$= [8]_5 = [5 \cdot 1 + 3]_5 = [3]_5$

Ex: $[3]_5 \cdot [4]_5 = [3 \cdot 4]_5$
$= [12]_5 = [5 \cdot 2 + 2]_5 = [2]_5$

Ex: Compute Cayley Tables for addition and mult. mod 6.

Sol:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	(3)	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
(2)	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Q: Why does this make sense?

i.e. Why are $+$ and $\cdot$ mod m "well-defined"?

Prop: Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ and $m \in \mathbb{Z}_+$. Assume $a_1 \equiv a_2 \bmod m$ and $b_1 \equiv b_2 \bmod m$.

① $(a_1 + b_1) \equiv (a_2 + b_2) \bmod m$

② $a_1 \cdot b_1 \equiv a_2 \cdot b_2 \bmod m$.

Exercise: prove this.

II. Greatest Common Divisors

Def^n: Let $a, b \in \mathbb{Z}$, not both zero. The greatest common divisor of a and b is

$$\gcd(a,b) := \max\{d \in \mathbb{Z} : d|a \text{ and } d|b\}.$$

($\max$: greatest; $d|a$ and $d|b$: d is a common divisor of a and b)

Ex: Compute $\gcd(10, 8)$ (via brute force).

Sol: Divisors of 10: $\pm 1, \pm 2, \pm 5, \pm 10$

Divisors of 8: $\pm 1, \pm 2, \pm 4, \pm 8$.

Common divisors: $\pm 1, \pm 2$ $\therefore \gcd(10, 8) = 2$.

Prop: Let $a, b \in \mathbb{Z}$ with $|a| \leq |b|$ (not both 0).

① If $|a| = |b|$, then $\gcd(a,b) = |a|$.

② If $a \neq 0$, then $\gcd(a,b) = \gcd(a,r)$ where $b \equiv r \bmod a$.

③ If $a = 0$, then $\gcd(a,b) = b$.

④ $\gcd(a,b) = \gcd(b,a)$.

pf: Let $a, b \in \mathbb{Z}$ w/ $|a| \leq |b|$ and $|b| \neq 0$.

①: Suppose $|a| = |b|$. Note $|a| \mid a$ and $|a| \mid b$ by basic properties of divisibility. Thus $\gcd(a,b) \geq |a| > 0$.

On the other hand, every common divisor of a and b is also a common divisor of $|a|$ and $|b|$. Thus every positive divisor of a, b is bounded above by $|a|$.

Hence $\gcd(a,b) \leq |a|$, so $\gcd(a,b) = |a|$ here.